

EXHIBIT A

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, S/A R.V. White, am a Special Agent with the North Carolina State Bureau of Investigation currently assigned to the Computer Crimes Unit. I have been a sworn law-enforcement officer in the State of North Carolina for approximately eighteen years. I have been employed with the North Carolina State Bureau of Investigation for approximately eighteen years.

In August 2003, I was hired by the North Carolina State Bureau of Investigation and received my Basic Law Enforcement Training Certification and attended the State Bureau of Investigation Academy; graduating in March 2004. After graduating from the SBI Academy I was assigned as the Resident Agent in the Rockingham and Caswell County, North Carolina. During my assignment in Rockingham and Caswell County, North Carolina, I conducted numerous investigations involving homicides, drug trafficking, public corruption, etc. In 2008, I was assigned as the Resident Drug Agent for Guilford County, North Carolina, I conducted numerous investigations involving drug trafficking until October, 2009. In October 2009, I was promoted to the Computer Crimes Unit with the duties of investigating computer crimes and internet crimes against children. Since being assigned to the Computer Crimes Unit, I have received training in undercover Peer 2 Peer internet investigations to include Gnutella, ARES, eMule, Bit Torrent and Freenet Networks. Computer forensic training includes EnCase I, II, Advanced Computer Forensics, Advanced Internet Examinations, Examinations of Macintosh and Linux Operating Systems, Basic Data Recovery and Acquisition (BDRA), Intermediate Data Recovery & Analysis (IDRA), Basic Investigation of Computer & Electronic Crimes Program (BICEP) taught by the United States Secret Service, Introduction to Digital Evidence Analysis (IDEA), Seized Computer Recovery Specialist (SCERS), Macintosh Forensic Training Program (MFTP) and Computer Network Investigations Training Program taught at the Federal Law Enforcement Training Center (FLETC).

As a Special Agent of the North Carolina State Bureau of Investigation, this Affiant is authorized to investigate crimes involving the sexual exploitation of children pursuant to North Carolina General Statute (NCGS) 14-190.17A.

NCGS 14-190.17A, known as Third Degree Sexual Exploitation of a Minor makes it unlawful for a person if, knowing the character or content of the material; he possesses material that contains a visual representation of a minor engaging in sexual activity.

NCGS 14-190.13, known as Definitions for Certain Offenses Concerning Minors provides the following definitions as applied to NCGS 14-190.17A, third degree sexual exploitation of a minor.

- A. Material. - Pictures, drawings, video recordings, films or other visual depictions or representations but not material consisting entirely of written words.
- B. Minor. - An individual who is less than 18 years old and is not married or judicially emancipated.
- C. Sexual Activity. - Any of the following acts:

- a. Masturbation, whether done alone or with another human or an animal.
- b. Vaginal, anal, or oral intercourse, whether done with another human or with an animal.
- c. Touching, in an act of apparent sexual stimulation or sexual abuse, of the clothed or unclothed genitals, pubic area, or buttocks of another person or the clothed or unclothed breasts of a human female.
- d. An act or condition that depicts torture, physical restraint by being fettered or bound, or flagellation of or by a person clad in undergarments or in revealing or bizarre costume.
- e. Excretory functions; provided, however, that this sub-subdivision shall not apply to G.S. 14-190.17A.
- f. The insertion of any part of a person's body, other than the male sexual organ, or of any object into another person's anus or vagina, except when done as part of a recognized medical procedure.
- g. The lascivious exhibition of the genitals or pubic area of any person.

The information contained within this affidavit is based upon information I have gained from my investigation, my personal observations, my training and experience, and/or information related to me by other law enforcement officers and/or agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are necessary to establish probable cause to believe that evidence of violations of North Carolina General Statute (NCGS) 14-190.17A is located at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina and/or within a computer and computer related storage media located within the business. Based upon the following information, there is probable cause to believe that at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina and /or within a computer and computer related storage media within the business which are suspected to contain images and movies depicting child pornography.

SEARCH AND SEIZURE OF COMPUTERS AND RELATED MEDIA

Based upon my training and experience and consultations with other law enforcement officers who have been involved in the search of computers and retrieval of data from computer systems, I know that searching and seizing information from computers often requires law enforcement officers to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. That process is lengthy and time consuming and takes days and even weeks. This is true because computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-ROMs) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to

conceal criminal evidence; he or she might store it in random order with deceptive file names. While an on-site computer preview is beneficial to get an initial glimpse of some of the items stored on the media, searching authorities will be required to examine all the stored data to determine which particular files is evidence or instrumentalities of a crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of full data search on site. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is often times difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

Therefore removal from the premises of some or all computer equipment and related storage media will be required for proper analysis and specific permission by this search and seizure warrant to remove the computer equipment and search it over time at a later date is sought.

BACKGROUND ON THE NETWORK

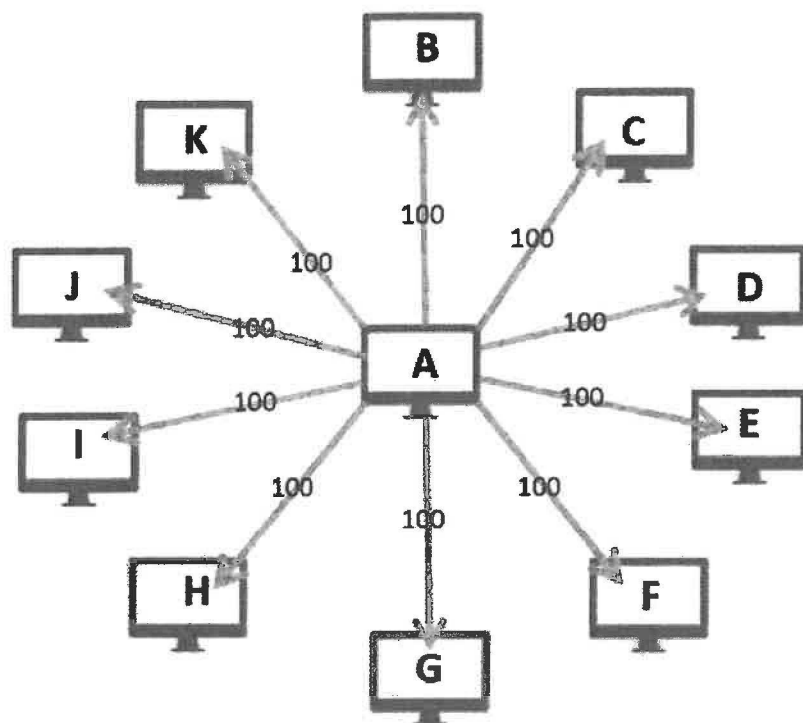
This case involves an Internet-based, peer-to-peer (P2P) network (the "Network") that allows users to anonymously share files, chat on message boards, and access websites. In order to access the Network, a user must first download the Network software, which is free and publicly available. Anyone running this software may join and access the Network. Each computer running Network software connects directly to other computers, which are called its "peers." When installing the Network software, each user agrees to provide to the Network a portion of the storage space on the user's computer hard drive, so that files uploaded by Network users can be distributed and stored across the Network. Network users can upload files into the Network and download files from the Network.

When a user uploads a file into the Network, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Network of peers.¹ The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file. In order to download a file, a Network user must have the key for the file.

When a user attempts to download a file via the Network, the Network downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Network software then requests all of the pieces of the file from the user's peers. Rather than request all of the file pieces from a single peer, requests for file

¹ Because the pieces of files are encrypted, a Network user is unable to access the content of pieces that are stored on the user's computer hard drive, which are not in a readable format.

pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on. For example, if User "A" has 10 peers and request 1000 pieces of a file, roughly 100 pieces are requested from each one of User A's peers. See figure 1.



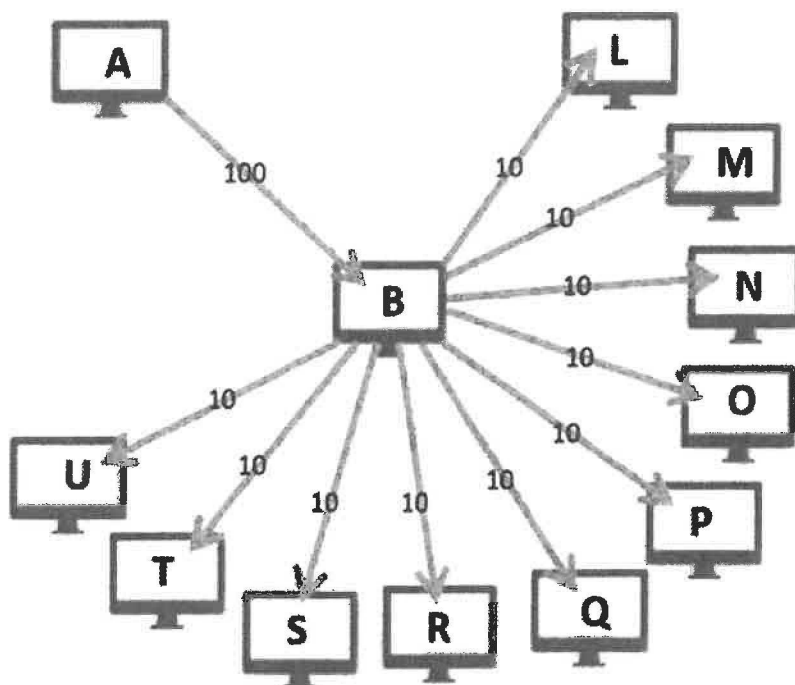
Network User A is connected to 10 peers.

User A wants to download a file that requires 1000 pieces to rebuild the file.

Because User A has 10 peers, roughly 100 pieces are requested from each one of User A's peers.

Figure 1

If Peer "B" receives User A's request for 100 pieces of the file, but does not have any of those pieces in its storage, Peer B forwards on the request for those pieces of Peer B's peers. If Peer B has 10 peers of its own, roughly 10 pieces are requested from each of the Peer B's peers. See Figure 2.



Peer B receives user A's request for 100 pieces of the file. Peer B does not have any of the pieces in its storage.

Peer B forwards on the request for pieces to each one of its peers.

Because B has 10 peers, roughly 10 pieces are requested from each one of B's peers.

Figure 2

This design can help law enforcement distinguish between a Network user that is the original requestor of a file, and one that is merely forwarding the request of another user. To prevent requests for pieces from going on indefinitely, the Network is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times. If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. The remaining number of times a request for a piece may be forwarded is included within the request for that piece.

The Network warns its users in multiple ways that it does not guarantee anonymity. Additionally, Network software does not mask a computer's IP address — the IP addresses of each user's peers are observable to the user. The Network also acknowledges on its publicly accessible website that it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers.

CHILD PORNOGRAPHY ON THE NETWORK

The Network can be used to advertise and distribute images and videos of child pornography. Unlike other file sharing systems, the Network does not provide a search function for its users whereby users conduct search terms to locate files. Therefore, a user who wishes to locate and download child pornography from the Network must identify the key associated with a particular child pornography file and then use that key to download the file.

Network users can identify those keys in a number of ways. For example, “message boards” exist on the Network which allows users to post messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: “pthc,” “boy porn,” “hussy,” “pedomom,” “kidfetish,” “toddler_cp,” “hurtcore,” and “tor-childporn.” Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through the Network, and in some cases descriptions of the image or video file associated with those keys.

Network users can also obtain keys of child pornography images or videos from websites that operate within the Network. These websites can only be accessed through the Network. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Network users may obtain keys related to child pornography images or videos directly from other Network users.

INVESTIGATION OF CHILD PORNOGRAPHY ON THE NETWORK

For some time now, law enforcement has been investigating the trafficking of child pornography on the Network. A modified version of the Network software is available to sworn law enforcement officers to assist in conducting Network investigations. This law enforcement version is nearly identical to Network software, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers.

Law enforcement computers do not target specific peers on the Network nor do law enforcement computers solicit requests from any peers. Network information collected by law enforcement computers is logged and provided to other trained law enforcement personnel in order to further investigations into Network users believed to be downloading child pornography files via the Network.

Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on the Network. Law enforcement only investigates Network users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Network message boards and websites, as well as during the course of prior investigations into child pornography trafficking on the Network.

By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. A mathematical formula is applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer.

SPECIFIC PROBABLE CAUSE

Your Affiant has reviewed information obtained and logged by law enforcement Network computers related to IP address 71.71.101.240. Such information shows that a Network user with

IP address 71.71.101.240 and with the Freenet Location ID 0.644952326875833, requested pieces of the child pornography files described below from a law enforcement Network computer. With respect to each file – considering the number of requested file pieces, the total number of file pieces required to assemble the file, and the number of peers the user had – the number of requests for file pieces is significantly more than one would expect to see if the user of IP address 71.71.101.240 were merely routing the request of another user. Accordingly – based on my review of those records, my understanding of the Network, my training and experience, and the fact that the same user requested pieces of multiple child pornography files – Your Affiant believes that the user of IP address 71.71.101.240 was the original requestor of each of the described files.

On Wednesday, September 22, 2021, while reviewing data received by law enforcement Freenet computers, your affiant observed IP address 71.71.101.240, with the Freenet Location ID 0.644952326875833, requesting blocks of suspected child pornography files. While it is not an absolute certainty the user was the original requestor, with respect to each file, considering the number of requested blocks, the total number of blocks required to assemble the file, and the number of peers the user had, the number of requests for blocks of the file is significantly more than one would expect to see if the user of IP address were merely routing the request of another user.

Between Monday, September 20, 2021 at 5:02 AM UTC and Monday, September 20, 2021 at 5:51 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 57.2 peers, requested from a law enforcement computer 146 out of 8,771 required pieces needed to assemble a file with a SHA1 digital hash value of GK7HLODTPFKAZOBR4NZKBSKJR2NJZCNX. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled “10yo Lilly likes anal.mp4”. The video is 29 minutes and 12 seconds in length. The video is of a prepubescent minor female approximately 9-11 years of age. The minor female begins the video wearing a shirt and a pair of panties. The minor female removes her panties exposing her vagina to the camera. The minor female begins rubbing her vagina with her fingers. The minor female retrieves a toothbrush and begins inserting the handle of the toothbrush in her anus. The minor female then retrieves the top of a baby’s bottle (the top with nipple) and begins inserting the bottle nipple in her vagina. The minor female then inserts the bottle nipple into her anus. The minor then removes the bottle nipple and begins sucking on it. The minor female continues inserting the bottle nipple in her vagina and anus throughout the rest of the video.

Between Monday, September 20, 2021 at 5:04 AM UTC and Monday, September 20, 2021 at 6:14 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 57.3 peers, requested from a law enforcement computer 113 out of 6,098 required pieces needed to assemble a file with a SHA1 digital hash value of DGFVMLX3AM5SF3J36KADZMEJYEOSU3EL. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled “caitlyn.mp4”. The video is 21 minutes and 6 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age. The minor female is lying nude on a bed with her legs spread apart and her vagina is exposed to the camera. The

minor female has an electric toothbrush and she is rubbing the toothbrush on her vagina. The minor female is also inserting the toothbrush into her vagina. The minor female begins rubbing her vagina with her fingers vigorously and inserting her fingers into her vagina. This continues throughout the video.

Between Monday, September 20, 2021 at 5:09 AM UTC and Monday, September 20, 2021 at 5:21 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 52.8 peers, requested from a law enforcement computer 23 out of 964 required pieces needed to assemble a file with a SHA1 digital hash value of I6AIWXZA6ZBLWW2UZSGLSGKQSRHKICZ5. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "Madison Cant Get a Break.mp4". The video is 8 minutes and 29 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age. The minor female removes her pants and exposes her vagina to the camera. The minor female begins rubbing her vagina with her fingers. The minor female continues exposing her vagina to the camera and spreading her vagina apart for the camera.

Between Monday, September 20, 2021 at 5:33 AM UTC and Monday, September 20, 2021 at 5:49 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 58.9 peers, requested from a law enforcement computer 55 out of 2,804 required pieces needed to assemble a file with a SHA1 digital hash value of VUVOTMWKIG3E5KRP3GA6QV4RMMSVOZ54. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "Arab_10yo_girl sex with man & boy.mpg". The video is 10 minutes and 2 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age and a minor prepubescent minor male approximately 7-10 years of age. The prepubescent minor female is engaged in sexual acts with an adult male. The prepubescent minor female and the prepubescent minor male engage in sexual acts with each other.

Between Monday, September 20, 2021 at 5:40 AM UTC and Monday, September 20, 2021 at 5:47 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 59.5 peers, requested from a law enforcement computer 36 out of 1,909 required pieces needed to assemble a file with a SHA1 digital hash value of CWCX2XNXMNRQC311P66FY6OHIGRIDWKG. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "12 year old asian fucked in the ass.mp4". The video is 1 minute and 9 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age. The minor female is lying face down on a bed. An adult male is behind the minor female between her legs. The adult male has his penis inserted in the vagina of the minor female. The adult male ejaculates on the buttocks on the minor female.

Between Monday, September 20, 2021 at 6:08 AM UTC and Monday, September 20, 2021 at 6:27 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 62.2 peers, requested from a law enforcement computer 46 out of 2,740 required pieces needed to assemble a file with a SHA1 digital hash value of HKGCNRKQP3QBX55TPDRT4LPCJVQTVUJK. Your affiant has downloaded the exact same

file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "a1122.avi". The video is 1 minute and 40 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age. The minor female is nude from the waist down and is sitting on the lap of an adult male who is also nude from the waist down. The adult male is inserting his penis in the vagina of the minor female.

Between Monday, September 20, 2021 at 6:14 AM UTC and Monday, September 20, 2021 at 6:47 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 62.9 peers, requested from a law enforcement computer 101 out of 5,729 required pieces needed to assemble a file with a SHA1 digital hash value of 5ZZXUX2XBAQWXWUT6L4DRLXT7Q2V2ZMH. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "anal 6yo brazilian.mp4". The video is 2 minutes and 31 seconds in length. The video is of a prepubescent minor female approximately 7-10 years of age. The minor female is lying nude on a bed. An adult male is between the legs of the minor female and has his penis inserted in the vagina and anus of the minor female throughout the video.

Between Monday, September 20, 2021 at 5:44 AM UTC and Monday, September 20, 2021 at 6:51 AM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 62.0 peers, requested from a law enforcement computer 169 out of 9,044 required pieces needed to assemble a file with a SHA1 digital hash value of MYXFV6TFMLMSX27RI57RSYDJJGVJJ5ZL. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "video_2021-08-24_20-37-05.mp4". The video is 29 minutes and 7 seconds in length. The video is of two prepubescent minor females approximately 7-10 years of age and an adult male. The adult male is videoed inserting his penis in the vagina of the minor females. The minor females are videoed inserting the adult male's penis into their mouths. The minor females are videoed using electric vibrators on their vaginas.

Between Sunday, October 17, 2021 at 5:03 PM UTC and Sunday, October 17, 2021 at 5:53 PM UTC, a computer running Freenet software with an IP address of 71.71.101.240, with an average of 56.0 peers, requested from a law enforcement computer 40 out of 2,822 required pieces needed to assemble a file with a SHA1 digital hash value of HIS6EI2WXGC3KPUCVV4XG4Y6ZQBDDH2J. Your affiant has downloaded the exact same file with the above referenced SHA1 hash value from the Network. The file with this digital signature is a video file entitled "Mandy mast part 2.mp4". The video is 13 minutes and 34 seconds in length. The video is of a prepubescent minor female approximately 7-9 years of age. The minor is sitting on a bed and begins to take off her shirt then her shorts and finally her panties. The minor female spreads her legs and exposed her vagina to the camera. The minor female leans back on the bed and spreads her legs further apart and begins spreading her vagina with her fingers. The minor female inserts her finger into her vagina. The minor female continues to lie on the bed exposing her vagina to the camera. The scene changes and the minor female is standing nude in a shower bathing.

The Network user has been observed requesting files associated with child pornography from 10/20/2020 to 10/17/2021 on the Freenet network.

The fact that a Network user requested pieces associated with a particular file on the Network indicates that the user attempted to download the file's contents from the Network. It does not indicate whether or not the user successfully retrieved all of the necessary pieces to successfully download the file.

The keys for each of these files were obtained by law enforcement agents at some point between 2011 and the present date either from a Network message board or Freesite that contained information related to the sexual exploitation of children, or from a previous investigation. Your Affiant is not aware of how, or from where, this particular Network user obtained a key in order to attempt to retrieve the files of interest described.

On September 22, 2021, an administrative subpoena was sent to Charter Communications to identify the subscriber of IP address 71.71.101.240.

On September 30, 2021, Charter Communications responded to the administrative subpoena and provided that the subscriber of IP address 71.71.101.240 was Rashawn McEachern residing at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina.

A TLO records check, which is a public records database showed Rashawn eric McEachern B/M/DOB: 11/05/1990 residing at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina 27302.

Based on my training and experience and the following court cases:

- A. United States v. Riccardi, 405 F.3d 852, 860-861 (10th Cir. 2005) (quoting United States v. Lamb, 945 F.Supp. 441, 460 (N.D.N.Y. 1996)) ("The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal courts: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.").
- B. United States v. Ricciardelli, 998 F.2d 8, 12, n. 4 (1st Cir. 1993). ("[H]istory teaches that collectors [of child pornography] prefer not to dispose of their dross, typically retaining obscene materials for years.");

it is probable that Mr. McEachern or someone associated at this location has built and maintained a collection of child pornography which he keeps with him where it is secure and readily accessible.

Based on the foregoing identification by IP address 71.71.101.240 and identification of child pornography files known to me, and the facts listed above there is probable cause to believe

that there is evidence of a continual pattern of on-going possession of child pornography through the Network (second degree sexual exploitation of a minor) (G.S. 14-190.17) located on the premises at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina. It is highly probable in my training and experience with this network that a user of the account identified by Charter Communications is active in possession of known or suspected child pornography on this network.

CONCLUSION

The Affiant has assisted in the execution of prior search warrants involving child pornography and digital evidence and P2P cases. In the prior cases, the computers were seized and found to contain trace evidence confirming the child pornography and P2P file sharing. In cases involving the same undercover techniques, experienced/seasoned agents have related that the information provided during the undercover operation had been confirmed through forensic examination and confessions.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that searches and seizures of evidence from computers require agents to seize most or all computer items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Computer storage media which can be accessed by computers to store or retrieve data or images of child pornography can store the equivalent of thousands of pages of information. This storage medium includes but is not limited to:

Floppy disks flash memory cards, compact flash cards and other similar storage medium, USB mini storage devices, micro hard drives, external hard drives internal hard drives, magnetic tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that searching computer systems for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), the controlled environment is essential to its complete and accurate analysis. The Affiant, or other assisting Internet Crimes against Children Task Force Officers, may however conduct a preview examination of the suspect's computer on-site using hardware and software that will not alter or change any potential evidence located on the suspect's computer.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that in order to fully retrieve data from a computer system, the examiner needs all digital storage devices as well as the computer. In cases like this one, where the evidence consists partly of graphic files, the input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media and the storage media are also essential to show the nature and quality of the graphic images which the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, user names or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

Based on your Affiant's training and consultation with experienced/seasoned agents, including computer forensic agents, who investigate child pornography cases, your Affiant knows that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child exploitation.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that files related to the exploitation of children found on computers are usually obtained from the Internet using application software

which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that computer software or hardware exists that allows persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of the Internet connection at the business.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of Internet service accounts used for the Internet access.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that search warrants of businesses involved in computer related criminal activity usually produces items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.

Based on your Affiant's training and consultation with experienced/seasoned agents that investigate child pornography cases, your Affiant knows that search warrants of businesses usually reveals items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

The above information has led the Affiant to believe that probable cause exists to believe that the items listed in the items to be seized sections of the search warrant application are evidence of the exploitation of children by means of the possession and attempted distribution of child pornography in violation of North Carolina General Statutes.

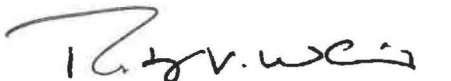
Pursuant to the execution of this search warrant, the Affiant and other assisting law enforcement officers will conduct a search of the business located at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina. Any evidence that is seized from the business will be analyzed forensically by Agents of the North Carolina State Bureau of Investigation Computer Crimes Unit or State Crime Laboratory personnel. This analysis will be primarily conducted off-site, from the property being searched, on a later date. The results of this analysis will be documented in a report included within an SBI investigative file. Depending on the scope of this search a portion of this analysis may (or may not) be conducted at the time the search warrant is executed.

Based on the investigation of the Network, IP address 71.71.101.240 was engaged in requesting to download child pornography computer files. Your Affiant's investigation determined that those files had SHA values associated with known or suspected child

pornography. Your Affiant determined, based on subpoenaed information that the IP address 71.71.101.240 was subscribed to Rashawn McEachern residing at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina, at the time that IP address 71.71.101.240 was requesting files with SHA values associated with known and suspected child pornography. Therefore, your Affiant believes that probable cause exists to search the business and the contents of digital media located at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina, for evidence of violations of G.S. 14-190.17A, known as Third Degree Sexual Exploitation of a Minor.

Therefore, this Affiant respectfully requests that a warrant be issued that authorizes affiant and officers to search the residence located at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina for the items listed in Attachment A which are evidence of violations of NC G.S. 14-190.17A.

In your affiant's training and experience with computers your affiant has found many computers (laptops) actually stored inside vehicles at the business and failure to check the vehicles would have resulted in not finding the computer at the business. In your affiant's training and experience the lease of the IP address is not always the one who used the computer on the network and frequently others in homes where an IP address is assigned can just as well be the perpetrator. As a result it is imperative to search for all computers in the business and or vehicles in order to determine who actually attempted to download child pornography files. It is highly probable in your affiant's training and experience with this network that an individual associated with the account identified by Charter Communications is active in the possession and downloading of child pornography on the Network. A search of that business where the Internet subscription comes back to, and the computers and routers at that business will reveal who at that business has been involved in active participation in possessing child pornography files.


Special Agent R.V. White


Superior Court Judge

Subscribed and sworn before me this ____ day of October, 2021.

ATTACHMENT A

ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense; or contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely a violation of NCGS 14-190.17A:

1. Computers and computer related storage media including, but not limited to, hard drives, thumb drives, CDs, DVDs, floppy disks, flash media, memory sticks, iPods, PDAs (Personal Digital Assistant), and other magnetic, digital, and/or optical recording media that are capable of storing digital files, to include images and videos.
2. Records evidencing use or moderation of a Gnutella P2P network including, but not limited to, screen names, filenames, digital pictures, dates/times of posted images, IP connection information related to the postings.
3. Graphic and movie files (including, but not limited to, files bearing file extensions .JPG, .GIF, .TIF, .AVI, and .MPG), and the data within the aforesaid objects relating to said materials, that depict child pornography.
4. Computer programs capable of viewing graphic files.
5. Text files containing information pertaining to the interest in child pornography or sexual activity with children and/or pertaining to the production, trafficking in, or possession of child pornography.
6. Correspondence, including, but not limited to, electronic mail, chat logs, and electronic messages, pertaining to the trafficking in, production of, or possession of visual depictions of minors engaged in sexually explicit conduct, as defined in NCGS 14-190.17.
7. Correspondence including, but not limited to electronic mail, chat logs, electronic messages, soliciting minors to engage in sexually explicit conduct for the purposes of committing an unlawful sex act and/or producing child pornography.
8. Names and addresses of minors visually depicted while engaged in sexually explicit conduct.
9. Files depicting sexual conduct between adults and minors.
10. Any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography.

11. Any and all documents and records pertaining to the purchase of any child pornography.
12. Notations of any password that may control access to a computer operating system or individual computer files, and/or that may indicate child pornography websites and passwords to those websites.
13. Evidence of payment for child pornography, including but not limited to: cancelled checks, money order receipts, or a debit entry in a computer software finance program or credit card statement.
14. Any child pornography in any form including, but not limited to, photographs, magazines, photocopies of photographs, videocassette tapes, and computer text or images.



Special Agent R.V. White

Subscribed and sworn before me this 20 day of October, 2021.



Superior Court Judge

ATTACHMENT B

DESCRIPTION OF PLACES TO BE SEARCHED

The residence located at 3051 Bluebird Lane, Apt 206, Mebane, North Carolina is a multi-family apartment complex. The building number 3051 is located on the side of the building. The apartment 206 is located on the second floor of the apartment complex. The Apartment #206 is located by the door to the apartment.



R. V. White

Special Agent R.V. White

Subscribed and sworn before me this 20 day of October, 2021.

Will A. Wood

Superior Court Judge